

## Information Management

Importance of data and information to organisations  
Key legislation affecting storage, communication & disposal of data & information

## Importance of data and information to organisations

- Qualities of information:
  - Completeness
  - Timeliness
  - Accuracy
  - Unbiasedness
  - Clarity
- Organisational goals explain how an organisation intends to go about achieving its mission
- The system goal explains the specific role of the information system in achieving the organisational goal.

## Storage, Communication & Disposal of information

- Legal obligations of an organization when:
- storing,
- communicating
- and disposing of data and information

## Information Privacy?

- The rights of individuals or organisations to disallow or restrict the use of information about them
- It has become more important due to the large amounts of personal data now being stored which has increased the potential for unauthorised use.

## Legislation: The Privacy Act 1988 (1)

- Act applies to Federal Government departments & private companies with a turnover of more than \$3million; can't give private information to anyone else.
- Doesn't apply to a health service or storage of health records
- Act applies to both electronic & manual forms of data gathering
- Act extends to workplace email
- Websites must display a privacy policy as do employers
- Key Principles: 11 key principles which can be summarised:
  - Data collection: information is collected in a manner that is lawful and those providing the information are informed as to the intended use of the information

## The Privacy Act 1988 (2)

- Data Processing, storage & maintenance:
  - Agencies have an obligation to ensure that information is accurate, up to date and complete
  - Individuals can access their own records and request alterations
  - Information that is stored is secure and has access restricted to those who have legitimate purposes
  - And is only kept for a time frame that is reasonable in the context of the purpose the data was collected for

### The Privacy Act 1988 (3)

- *Data Use:*
  - Data can only be used for the purpose it was collected
  - Any other use must be accompanied by the consent of the individual it was collected from
  - Unless there is threat to life or health or in the enforcement of the law

### The Information Privacy Act (Vic)

- The Act provides the same protection as the Privacy Act 1988; based on set of 10 principles
- The Privacy Act 1988 deals with Comm. Govt. Agencies & Private org.
- The Information Privacy Act (Vic) deals with the Vict. Govt. departments, Agencies & their sub contractors as well as Vict. Local govt. bodies

### The Information Privacy Act (Vic) (2)

- If the organisation in question is a Vict. Govt. Agency, local council or a sub contractor of them, then they will be covered by the Act
- All other organisations are covered by the Comm. Act
- A function of the Act is to establish the office of the Victorian Privacy Commissioner to oversee the compliance with the act
- Penalties: compliance notice issued to organisations; maximum penalties, \$100,000

### The Health Records Act 2001 (Vic)

- This act covers both the govt. and private medical sectors & details the rights of individuals & the responsibilities of organisations that hold information
- It allows a greater level of exemptions and exclusions than other privacy legislation; eg. Requests by family members in an emergency when you can't give your consent & your life is threatened, serious threat to public health & welfare, research in the public interest, investigation of unlawful activity and as part of a legal claim.

### The Health Records Act 2001 (Vic) (2)

- It allows people to access their own medical information
- Health privacy principles based on the 11 information privacy principles
- Health information can only be used for the primary purpose for which it was gathered, eg. Not disclosed to a third party, eg. Medical insurance company.
- It also covers in greater detail the manner in which information can be used, especially in research
- Established a Health Services Commissioner
- Maximum penalty for an organisation is \$300,000 and \$60,000 for non-corporate cases.

### Copyright Act 1968; Copyright Amendment (Digital Agenda) Act 2000, Copyright Amendment Act 2006 & Australia-United States Free Trade Agreement, (AUSFTA).

- What is copyright?
  - The legal protection of an Idea against copying or use without permission.
  - In Australia copyright protection is automatic, it doesn't need to be registered.
  - It has become important with the advent of the internet and cable TV where many items are easily copied.
  - Intellectual property, "product of human thought", texts, videos, music, broadcasts & computer games
  - Does not cover ideas, concepts, styles, techniques, slogans
  - Copyright infringed if materials is used without permission
  - Updated to cover work published electronically; work produced, stored or transmitted digitally
  - Copyright applies for the life of the creator plus 70 years

### Copyright Act 1968; Copyright Amendment (Digital Agenda) Act 2000, contd

- Who Owns Copyright
  - General rule is that the creator of the item is 1st owner
  - The right can be varied by agreement but there are some significant exclusions
  - When the work is made by an employee in the course of employment and as a part of the employee's usual duties then the 1st owner of copyright is the employer
  - This includes programs/websites/docs. etc. written by employee
  - Doesn't include if written in freelance or contract arrangement

### Copyright Act Contd

- Exceptions where permission from copyright owner is not required:
  - Making a backup copy of computer program
  - Can lend a legitimate copy of a game to someone to play but it is illegal to play an infringing copy; (b/c reproduced)
  - Can make copies of works purchased and transfer them into other formats for personal use, eg. From CD to a MP3 format
  - Government use "for the services of government"
  - Can access some legitimate copyright material, such as time-shift recordings
  - Penalties: Fines up to \$93500 for an individual and/or 5 yrs jail
  - An organisation may face up to 5 times the individual amount

### Charter of Human Rights and Responsibilities

- Australia supports and accepts United Nations human rights principles.
- Victorian legislation provides protection of rights such as:
  - Freedom of expression
  - Privacy and reputation
  - Freedom of thought, conscience, religion and belief

### Spam Act 2003

- Spamming: posting undesirable messages to newsgroups and mailing lists or sending unsolicited email indiscriminately to promote a product or service, junk mail.
- Spamming involves costs to businesses and end users; obstructing legitimate business activities
- Spam Act promotes responsible use of sending commercial electronic messages and send must identify themselves; must have the recipient's consent and also provide the recipient with a method to unsubscribe if they wish
- Spam Act covers only commercial messages; sent using electronic applications, eg. email; SMS, MMS and iM.
- Spam Act doesn't cover non-electronic messages, eg. ordinary mail or voice-to-voice telemarketing
- Penalties: a business in breach, up to \$220000; or if breach again, up to \$1.1 m.

## Storage, Communication & Disposal of data & information

Threats to data & Information  
Deliberate, accidental & technical failure

### Deliberate threats

- Intentional Damage
  - Computer viruses, payload is the action virus designed to carry out
    - Worms, attaching themselves to email messages, clog servers
    - Viruses prevents computer from running executable files, destroy data
    - Viruses mainly spread through email file attachment or transfer of infected files
    - Macro is most common form of virus
  - Hacking/Cracking
    - Hackers gain unauthorised access and view data but not tamper

### Security, Intentional Damage

- Tampering with files
  - Crackers
  - Files changed by personnel with access rights who sell information to others
  - Files intercepted whilst being transmitted
- Theft of information & hardware & vandalism

### Security, Accidental damage

- User error
  - Copying older version of file over newer version
  - Formatting a disk containing data
  - Not correctly shutting down hardware
  - Failure to follow file-management procedures
    - Descriptive filenames
    - File extensions left off
    - Folders improperly used
  - Equipment failure/damage

### Technical Failure

- Examples of:
  - Hard disk fails
  - Operating system not working properly
  - Damage by electricity
  - Fire, smoke, water
  - breakage

### Consequences of data security violation and privacy measures

- Consequences of data security violation
  - Breaches of privacy
  - Loss of intellectual property
  - Loss of income

## Security Equipment

Equipment for preventing unauthorised access to data & information

## Security Equipment, Hardware

- Biometrics
  - Authentication based on what you are (Biometrics)
  - Biometrics, human recognition: Physical traits unique to each individual
    - Biometric scanning: whereby biometric measurements are collected and integrated into a computer system. Used for two purposes:
      - identification, "Do I know you", one-to-many match
      - authentication "Are you who you claim to be", 1-1 match

## Biometrics contd

- Biometric devices:
  - Voice recognition
  - Fingerprint recognition
  - Hand geometry
  - Signature verification
  - Facial recognition
  - Iris recognition

## Biometrics contd

- Advantages:
  - recognition based on an intrinsic aspect of a human
  - non-intrusive data collection
  - no or minimal contact between person and scanning equipment
  - automated
  - high accuracy, high speed
  - minimal training



## Biometrics contd

- Disadvantages; depending on type of technology
  - need for close physical contact with scanner
  - user acceptance, intrusiveness of technology
  - expense of system
  - memory intensive storage requirements
  - Common biometric devices:
    - Voice recognition; fingerprint recognition; hand geometry; signature verification; facial recognition; iris recognition.

## Equipment, Swipe Cards

- Swipe Cards
  - Electronic transactions; eg. credit cards, ATM cards
  - Internal security within organisation, also hotels
  - Limitation:
    - Easily damaged by magnetic fields
    - If stolen, little protection

### Equipment, Smart Cards

- Smart card,
  - embedded microchip which stores and manipulates data, eg. telstra telephone card, photocopy cards, Myki public transport ticketing system
- Security tokens
  - Two-factor authentication; enter a/c name & p/word and authentication code on security token
  - If lose token can't access data either
- Mobile phone secure code
  - Authentication occurs when a security code is sent to the account holder's mobile phone to authenticate a transaction before it actually occurs.

### Equipment, Power protection

- Surge protector
  - protects electrical equipment against overvoltage caused by a power surge
- UPS, used in server rooms;
  - high quality surge protector & battery;
  - Protect data if there is an undercurrent or complete power failure
  - As soon as loss of power to UPS, batteries begin to supply power

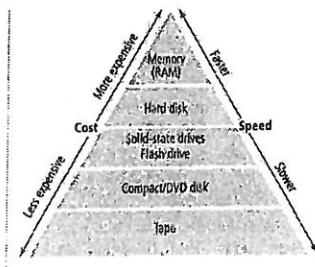
### Strategies for avoiding system failure

- Redundancy, no single part of the system is critical to its overall operation; if one part fails, the others, hard drives or mirrored machines take over; also know as fault tolerant systems
- 1 Redundancy through multiple hard drives
    - Continuously copy data onto a second, "mirrored" hard drive; if main drive fails, then a duplicate set of data is available on mirrored drive
    - Use of a RAID system; data spread over several hard drives; requires a controller and disk drives
  - 2 Redundancy through mirrored servers
    - More expensive than above b/c requires extra hardware

### Equipment, Backup media

- Operating systems contain built-in-backup utility
- In deciding which device to use consider:
  - Cost of drive or writer
  - Cost of media per MB or GB
  - Speed &
  - Compatibility
  - Issue of support in years to come

### Storage media & memory, terms of cost & speed



### Equipment, Backup media

- Magnetic Media
  - Hard disk drive, any size; common in schools
  - Magnetic tape
    - Relatively cheap but slow to save & restore files, sequential access.
- Optical Drives
  - CD ROM, (700 mb); DVD, 17 gb double sided
  - Blu-ray, 50gb (dual layer); 5 times more storage than DVD and allows high definition films to be stored.
- Solid-state drives
  - USB storage devices; convenient, no moving parts, less chance of breakdown, store 2 gb of data

### Equipment, Online backups

- Use of remote servers via internet
  - Organisations want to consolidate storage & backup systems to ensure they work with access to fault tolerant servers, UPS, etc.
- Enterprise storage systems
  - Use of a storage area network, (SAN) of RAID disks, tapes, CD/DVD-ROM servers, internet backups & other networked storage devices

### Enterprise storage system

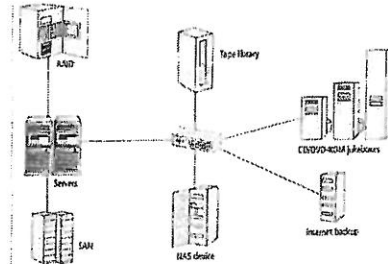


FIGURE 6-9  
An enterprise storage system uses a variety of storage techniques to ensure its data is secure.

### Surveillance technology

- Packet sniffers, (for internet & email)
  - Diagnostic tools monitoring contents of data sent across networks
  - Used to monitor email & internet usage
- Desktop monitoring programs
  - See what is on the desktop
  - All tasks are logged
  - Hackers use these applications
- Log Files
  - Webservers record every URL accessed, web browsers store webpages, networks, etc.

### Surveillance technology

- CCTV
- Telephones
- Audit Trails
  - Log files of system logins
  - Files accessed modified or copied

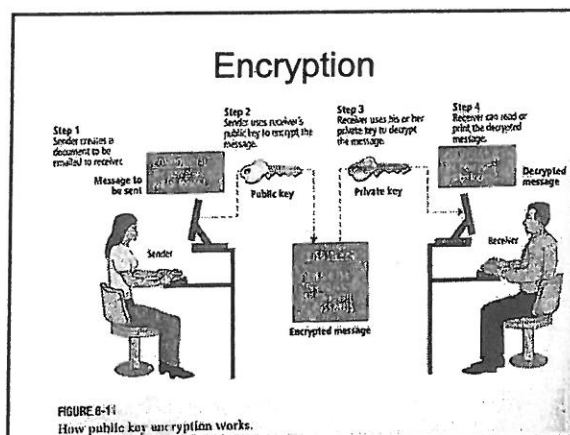
### Security, Physical security devices

- Lockable disk box
- Safe or specialised room
- Security cables attached to items

## Security: Software & procedures

## Security, Software

- Encryption: two types:
  - Symmetric-key encryption, sender & receiver have the same key installed on their computers
  - Asymmetric-key encryption, (public-key encryption)
  - Sender encrypts message or file using recipient's public key
  - Recipient decrypts using their private key



## Security, Software

- Network policies & procedures
  - Authentication, password
  - Characteristics of a good password
  - Authorisation & permissions on a network
- Firewalls
  - Restrict access to a network from outsiders and from insiders to certain information
  - Combination of hardware and/or software
  - Also provide protection against viruses & hackers

## Security, Software

- Anti-virus software
  - Update as often as available
  - Scan for virus signatures

## Security Procedures

- Organisations require policies to define how an information system should be used.
- Communication
  - Faxes
  - Email
    - Conventions: subject heading & message priority; signature of person sending it; privacy disclaimer at end of email; use of appropriate language; attachments sent in appropriate format



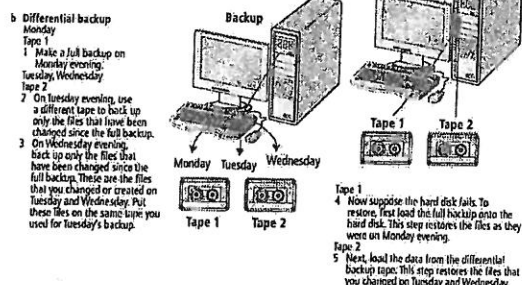
## Security Procedures

- Storage
  - File-naming conventions:
    - Include datestamp, eg. newsletter 2006-11.doc
    - Variation, newsletter 2006-11 v3.doc
    - Sequential file-naming convention, newsletter 2006-11 03oct.doc
    - Name, meaningful
  - Location of files
    - Use of a directory structure

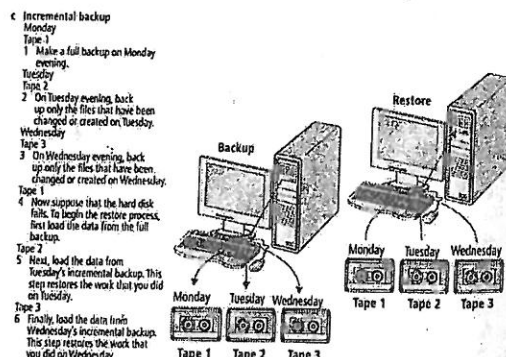
## Security Procedures

- Storage
  - Backups:
    - Full backup, all files
    - Differential backup, files that have changed since last full backup, uses only 2 media
    - Restoration of files involve restoring files from the full backup and then from the differential backup
    - Incremental backup, files changed only back up data that has changed since the last incremental backup
      - Smaller, faster than differential
      - Incremental backups give much greater flexibility they take longer to restore because the backup has to be reconstituted from the last full backup and all the incremental backups since.

## Differential Backup



## Incremental Backup

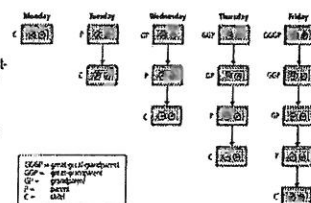


## Security Procedures

- Storage
  - Backups:
    - Backup logs
    - Restoration logs
    - Volume name or number; where the backup data has come from.

## Security Procedures

- Backup timeline
  - Grandparent-parent-child system
  - Incremental backup each day
  - Differential backup at end of each week
  - Full backup end of each month



**FIGURE 5-18**  
A suggested backup routine known as the grandparent-parent-child system. The parent is the second oldest copy of the file. The child is the most recent copy of the file. An incremental backup is performed each day with a differential backup at the end of each week. A full backup is done at the end of each month.

### Security Procedures

- Location of backup files
  - Fireproof & waterproof safe
  - Remote location, eg. another city
  - Off-site backup storage
  - Test backups

### Security Procedures

- Archiving/destruction
  - Legal reasons
  - Stored on same type of media as backups
  - Stored in similar locations
  - Legacy system; an old system, eg. running old databases on old servers or mainframes.
- Disposal
  - Policies required for disposal

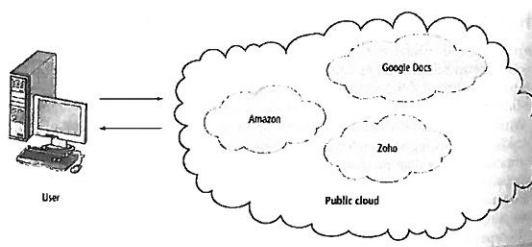
## Cloud Computing

The advantages and disadvantages of using cloud computing for storing, communicating and disposing of data and information.

## Cloud Computing Characteristics

- A service provided by large internet-based specialised data centres that offers storage, processing and computer resources to individuals and organisations.
- The services are shared, on-demand and simple to use.
- Pay for use and as needed, elastic (scale up and down in capacity and functionalities); "always on!"
- The "no-need-to-know" in terms of the underlying details of infrastructure, applications interface with the infrastructure via the APIs.
- Eg. Google's gmail uses cloud computing processing powers and storage facilities; Zoho offers tools to businesses including web conferencing, applications and project-management tools.

## Cloud Computing



Public Cloud, where a business can access web services via a third party.

## Cloud Computing: Types of:

- Public cloud, business accesses web services via a third party who shares resources & costs on a utility or use base
- Community cloud, group of organisations with similar needs seek to share the infrastructure; eg. group of finance companies with a higher level of security demands
- Hybrid cloud, business accessing a mix of cloud services in a public & community environment
- Private cloud, tailored to suit private client, eg. wanting higher levels of security, eg. medical institutions.

## Different Cloud Computing Layers

<b>Application Service (SaaS)</b>	MS Live/ExchangeLabs, IBM, Google Apps; Salesforce.com, Quicken Online, Zoho, Cisco
<b>Application Platform</b>	Google App Engine, Mosso, Force.com, Engine Yard, Facebook, Heroku, AWS
<b>Server Platform</b>	3Tera, EC2, SliceHost, GoGrid, RightScale, Linode
<b>Storage Platform</b>	Amazon S3, Dell, Apple, ...

## Advantages of Cloud Computing

- Scalability
  - The ability of the platform to expand and contract automatically based on capacity needs (sometimes referred to as "elasticity"); The on-demand nature of cloud computing means that as your demand grows (or contracts) you can more easily match your capacity (and costs) to your demand
- Lower costs: Don't need:
  - high-powered and high-priced computer to run cloud computing's web-based applications.
  - Since applications run in the cloud, not on the desktop PC, your desktop PC does not need the processing power or hard disk space
  - technical personnel necessary to keep a data centre up and running
  - utility bills and capital expense investments for power and cooling
  - contract and account people to keep track of all the various licenses, leases, etc.
  - When you are using web-based applications, your PC can be less expensive
  - Reduced software costs

### Advantages of Cloud Computing

- Instant software updates:
  - Another advantage to cloud computing is that you are no longer faced with choosing between obsolete software and high upgrade costs.
  - When the application is web-based, updates happen automatically - available the next time you log into the cloud.
  - When you access a web-based application, you get the latest version - without needing to pay for or download an upgrade.
- Improved document format compatibility.
  - You do not have to worry about the documents you create on your machine being compatible with other users' applications or operating systems.
  - Where Word 2007 documents cannot be opened on a computer running Word 2003, all documents can be read!
  - There are potentially no format incompatibilities when everyone is sharing documents and applications in the cloud.

19th May, 09

mark.baker@computer.org

### Advantages of Cloud Computing

- Unlimited storage capacity:
  - Cloud computing offers virtually limitless storage.
  - Your computer's current 200 Gbyte hard drive is small compared to the hundreds of Pbytes available in the cloud.
  - Whatever you need to store, you can.
- Increased data reliability:
  - Unlike desktop computing, in which if a hard disk crashes and destroy all your valuable data, a computer crashing in the cloud should not affect the storage of your data.
  - That also means that if your personal computer crashes, all your data is still out there in the cloud, still accessible.
  - In a world where few individual desktop PC users back up their data on a regular basis, cloud computing is a data-safe computing platform!

### Advantages of Cloud Computing

- Easier group collaboration:
  - Sharing documents leads directly to better collaboration.
  - Many users do this as it is an important advantages of cloud computing - multiple users can collaborate easily on documents and projects.
  - Because the documents are hosted in the cloud, not on individual computers, all you need is an Internet connection, and you are collaborating.
- Device independence.
  - You are no longer tethered to a single computer or network.
  - Changes to computers, applications and documents follow you through the cloud.
  - Move to a portable device, and your applications and documents are still available.

19th May, 09

mark.baker@computer.org

### Advantages of Cloud Computing

- Universal document access:
  - That is not a problem with cloud computing, because you do not take your documents with you.
  - Instead, they stay in the cloud, and you can access them whenever you have a computer and an Internet connection.
  - All your documents are instantly available from wherever you are.
- Latest version availability:
  - Another document-related advantage of cloud computing is that when you edit a document at home, that edited version is what you see when you access the document at work.
  - The cloud always hosts the latest version of your documents; as long as you are connected, you are not in danger of having an outdated version.

### Advantages of Cloud Computing- Key word

- CASHMEC
- C, Costs of software, hardware
- A, Anywhere any time access
- S, Storage and security
- H, Hardware scalability
- M, no maintenance, less IT staff
- E, Easy to use
- C, Collaboration

### Disadvantages of Cloud Computing

- Requires a constant Internet connection:
  - Cloud computing is impossible if you cannot connect to the Internet.
  - A dead Internet connection means no work and in areas where Internet connections are few or inherently unreliable this is a problem
  - When you are offline, cloud computing simply does not work.
  - Need to install redundant internet connections

### Disadvantages of Cloud Computing

- Does not work well with low-speed connections:
  - Similarly, a low-speed Internet connection, such as that found with dial-up services, makes cloud computing painful at best and often impossible.
  - Web-based applications require a lot of bandwidth to download, as do large documents.
- Can be slow:
  - Even with a fast connection, web-based applications can sometimes be slower than accessing a similar software program on your desktop PC.
  - Everything about the program, from the interface to the current document, has to be sent back and forth from your computer to the computers in the cloud.

11:15 May '09

mark.baker@computer.org

### Disadvantages of Cloud Computing

- Software capabilities
  - This situation is bound to change, but today many web-based applications simply are not as full-featured as their desktop-based applications.
  - For example, you can do a lot more with Microsoft PowerPoint than with Google Presentation's web-based offering.
- Availability & Service Levels
  - One of the most common concerns regarding cloud computing is the potential for down-time if the system isn't available for use.

11:15 May '09

mark.baker@computer.org

### Disadvantages of Cloud Computing

- Stored data might not be secure:
  - With cloud computing, all your data is stored on the cloud.
  - Can unauthorised users gain access to your confidential data?
  - Cloud computing companies say that data is secure, but it is too early to be completely sure of that.
  - Only time will tell if your data is secure in the cloud.
- Stored data can be lost:
  - Theoretically, data stored in the cloud is safe, replicated across multiple machines.
  - But on the off chance that your data goes missing, you have no physical or local backup.
  - Put simply, relying on the cloud puts you at risk if the cloud lets you down.

### Disadvantages of Cloud Computing- Key word

PADDLLSSC  
 P, Privacy  
 A, Availability and speed of connection  
 D, Data loss  
 D, Data ownership  
 L, Lack of control  
 L, Legal issues, operate in different countries  
 S, Staff, training of staff  
 S, Software capabilities, less features than desk top application  
 C, Cost of purchasing service

## Ethical dilemmas arising from information management strategies used by organisations

Ethics & Information Systems

## Ethics & Information Systems

- Ethics, What are they?
  - Moral principles or guidelines that govern particular practices or actions.
  - Whilst morally questionable, not against the law
  - Eg. violent video games; principle of protecting children Vs freedom of expression

## Ethics & IS

- Workplace responsibilities, both employer & employee
  - Employee expected to work in interests of employer
  - Organisation expected to provide good quality products & high quality service
- Codes of conduct & computer user policies
  - Code of conduct, - behavior expected of employee
  - Computer use policy, establishing rights & responsibilities of employees

## Ethics & IS

- Employee monitoring
  - Rights of employers Vs privacy of employee
  - Monitoring email
  - Advantages:
    - Ensures employees are doing company work
    - Ensures employees maintain target performance levels
    - It saves time and money
  - Disadvantages:
    - It is intrusive and may impact on employee privacy
    - Mistrust may develop b/w employee and employer
  - Web browsing monitored by automatic logs
  - Use of cookies to store history

## Ethics & IS

- The internet
  - Netiquette; network etiquette
    - means of regulating internet publishing
    - Eg. not posting to inappropriate groups
    - Personal messages to one or two individuals should not be posted to newsgroups.
  - Spamming, sending unsolicited email;

## Resolving legal, ethical & social tensions

- Legislation exists, eg. Copyright Act & Privacy Act
- Organisations have policy documents that mandate who has access to areas of the IS
- Six steps framework for handling ethical dilemmas
  - Identify the problem
  - Identify the stakeholders
  - Identify possible alternatives
  - Identify ethical standards
  - Evaluate options
  - Make a decision
  -

## Disaster Recovery Strategies & criteria for evaluation of information management strategies

## Disaster Recovery Strategies

- A document with steps needed to restore company operations in event of a disaster
- Four key parts:
  1. Emergency Plan
    - Names & contact details of people to notify
    - Procedures to follow with computer equipment
    - Evacuation procedures for employees
    - Return procedures

## Disaster Recovery Strategies

- 2 Backup Plan
  - Location of alternative sites & equipment
  - Location of backup data, supplies, eq/ment
  - Personnel responsible for gathering backup resources
  - Schedule indicating order & approximate time applications up and running

## Disaster Recovery Strategies

- 3 Recovery Plan
  - Covers hardware & software replacement
  - Identification of mission critical ICT services
  - Use of a backup site
- 4 Test Plan
  - Simulation of variety of disasters & recovery needs

## Evaluating the effectiveness of data security measures

- Integrity of data
  - accuracy, reliability and timeliness in terms of storage, communication and disposal
  - Accuracy, eg. storage, it contains all data; communication, arrives accurately, no viruses; disposal, selected files deleted or copied
- Security
  - Evaluate physical & software security, eg. audit trails

## Evaluating the effectiveness of data security measures

- Ease of retrieval
  - Observance of folder & file-naming conventions
  - Backed up files need to be able to be restored
- Currency of files
  - Regular backups
  - Use of sequential file-naming conventions

